F5 BIG-IP Systems: Integration Guide

THALES LUNA HSM AND DPOD LUNA CLOUD HSM

Document Information

Document Part Number	007-000265-001
Revision	D
Release Date	25 January 2021

Trademarks, Copyrights, and Third-Party Software

CONTENTS

Overview

This document contains steps for configuring F5 BIG-IP Systems and integrating them with Luna HSM devices or Luna Cloud HSM services. The BIG-IP LTM system uses the Luna HSM to generate and secure the keys used by the Secure Sockets Layer (SSL). You can use the Luna HSM solution with all BIG-IP platforms, including VIPRION Series chassis and appliances and BIG-IP Virtual Edition (VE). With Luna Network HSMs, you can also configure multiple HSMs as an HA (high availability) group to use with BIG-IP systems.

> **NOTE:** The BIG-IP system, when in appliance mode, does not support Luna Network HSM installation/uninstallation as the user needs root privilege for that.

In BIG-IP system, RSA-based cipher suites and ECDHE-ECDSA cipher suites use the Luna HSM. After installation on the BIG-IP system, the Luna HSM is compatible with Access Policy Manager and Application Security Manager without additional configuration steps.

The benefits of securing the CA key with Luna HSM include:

- Secure generation, storage, and protection of the signing private key on FIPS 140-2 level 3 validated hardware.
- Full life cycle management of the keys.
- Access to the HSM audit trail*.
- The ability to use cloud services with confidence.

*Luna Cloud HSM services do not have access to the secure audit trail.

Certified Platforms

HSM Type	F5 BIG-IP LTM
Luna HSM	14.1 14.0

Luna HSM: Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. Luna HSM on premise offerings include the Luna Network HSM, Luna PCIe HSM, and Luna USB HSMs. Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

> **NOTE:** This integration is tested with Luna HSM in HA & FIPS Mode.

HSM Type	F5 BIG-IP LTM
Luna Cloud HSM	14.1

Luna Cloud HSM : Luna Cloud HSM provides on-demand HSM and Key Management services through a simple graphical user interface. With Luna Cloud HSM, security is simple, cost effective and easy to manage because there is no hardware to buy, deploy and maintain. As an Application Owner, you click and deploy services, generate usage reports and maintain just the services you need.

Prerequisites

Before you proceed with the integration, complete the following tasks:

Configure Luna HSM

If you are using Luna HSM:

1. Verify the HSM is set up, initialized, provisioned and ready for deployment. Refer to the Luna HSM documentation for more information.
2. Create a partition that will be later used by F5 BIG-IP.
3. If using a Luna Network HSM, register a client for the system and assign the client to the partition to create an NTLS connection. Initialize the Crypto Officer and Crypto User roles for the registered partition.
4. Ensure that the partition is successfully registered and configured. The command to see the registered partitions is:

```
/usr/safenet/lunaclient/bin/lunacm

lunacm (64-bit) v10.2.0-111. Copyright (c) 2020 SafeNet. All rights reserved.

Available HSMs:

Slot Id ->              0

Label ->                bigip

Serial Number ->        1280780175877

Model ->                LunaSA 7.3.0

Firmware Version ->     7.3.0

Configuration ->        Luna User Partition With SO (PW) Key Export With
Cloning Mode

Slot Description ->     Net Token Slot

FM HW Status ->         FM Ready
```

5. For PED-authenticated HSM, enable partition policies 22 and 23 to allow activation and auto-activation.

> **NOTE:** Refer to the Luna HSM documentation for detailed steps on creating NTLS connection, initializing the partitions, and assigning various user roles.

Set up Luna HSM High-Availability

Refer to the Luna HSM documentation for HA steps and details regarding configuring and setting up two or more HSM boxes on host systems. You must enable the HAOnly setting in HA for failover to work so that if the primary goes down due to any reason all calls automatically route to the secondary until the primary recovers and starts up.

Set up Luna HSM in FIPS Mode

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the Luna HSM in FIPS mode, you have to make the following change in the configuration file:

```
[Misc]
RSAKeyGenMechRemap=1
```

The above setting redirects the older calling mechanism to a new approved mechanism when Luna HSM is in FIPS mode.

> **NOTE:** The above setting is not required for Universal Client. This setting is applicable only for Luna Client 7.x.

Configure Luna Cloud HSM Service

You can configure Luna Cloud HSM Service in the following ways:

> Standalone Cloud HSM service using minimum client package

> Standalone Cloud HSM service using full Luna client package

> Luna HSM and Luna Cloud HSM service in hybrid mode

> **NOTE:** Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

Standalone Cloud HSM service using minimum client package

To configure Luna Cloud HSM service using minimum client package:

1. Transfer the downloaded .zip file to your Client workstation using pscp, scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

   ```
   [Linux]

   cvclient-min.tar

   # tar -xvf cvclient-min.tar
   ```

4. Run the setenv script to create a new configuration file containing information required by the Luna Cloud HSM service.

   ```
   [Linux]
   ```

   ```
   Source the setenv script.
   ```

   ```
   # source ./setenv
   ```

Run the LunaCM utility and verify the Cloud HSM service is listed.

Standalone Cloud HSM service using full Luna client package

To configure Luna Cloud HSM service using full Luna client package:

1. Transfer the downloaded .zip file to your Client workstation using pscp, scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

   ```
   [Linux]
   ```

   ```
   cvclient-min.tar
   ```

   ```
   # tar -xvf cvclient-min.tar
   ```

4. Run the setenv script to create a new configuration file containing information required by the Luna Cloud HSM service.

   ```
   [Linux]
   ```

   ```
   Source the setenv script.
   ```

   ```
   # source ./setenv
   ```

5. Copy the server and partition certificates from the Cloud HSM service client directory to Luna client certificates directory:

   > **NOTE:** Skip this step for Luna Client v10.2 or higher.

   Cloud HSM Certificates:

   ```
   server-certificate.pem
   ```

   ```
   partition-ca-certificate.pem
   ```

   ```
   partition-certificate.pem
   ```

   LunaClient Certificate Directory:

   ```
   [Linux default location for Luna Client]
   ```

   ```
   /usr/safenet/lunaclient/cert/
   ```

6. Open the configuration file from the Cloud HSM service client directory and copy the XTC and REST section.

   ```
   [Linux]
   ```

   ```
   Chrystoki.conf
   ```

7. Edit the Luna Client configuration file and add the XTC and REST sections copied from Cloud HSM service client configuration file.

8. Change server and partition certificates path from step 5 in XTC and REST sections. Do not change any other entries provided in these sections.

> **NOTE:** Skip this step for Luna Client v10.2 or higher.

[XTC]

```
. . .
PartitionCAPath=<LunaClient_cert_directory>\partition-ca-certificate.pem
PartitionCertPath00=<LunaClient_cert_directory>\partition-certificate.pem
. . .

[REST]
. . .
SSLClientSideVerifyFile=<LunaClient_cert_directory>\server-certificate.pem
. . .
```

9. Edit the following entry from the Misc section and update the correct path for the plugins directory:

```
Misc = {
...
PluginModuleDir=<LunaClient_plugins_directory>;
...
}
```

```
[Linux Default]
```

```
/usr/safenet/lunaclient/plugins/
```

Save the configuration file. If you wish, you can now safely delete the extracted Cloud HSM service client directory.

10. Reset the ChrystokiConfigurationPath environment variable and point back to the location of the Luna Client configuration file.

Linux

Either open a new shell session, or export the environment variable for the current session pointing to the location of the Chrystoki.conf file:

```
# export ChrystokiConfigurationPath=/etc/
```

11. Run the LunaCM utility and verify that the Cloud HSM service is listed. In hybrid mode, both Luna and Cloud HSM service will be listed.

> **NOTE:** Follow the Luna Cloud HSM documentation for detailed steps for creating service, client, and initializing various user roles.

Luna HSM and Luna Cloud HSM service in hybrid mode

To configure Luna HSM and Luna Cloud HSM service in hybrid mode, follow the steps mentioned under the Standalone Cloud HSM service using full Luna client package section above.

> **NOTE:** Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

Use Luna Cloud HSM Service in FIPS mode

Cloud HSM service operates in both FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, enable the Allow non-FIPS approved algorithms check box when configuring your Cloud HSM service. The FIPS mode is enabled by default. Refer to the Mechanism List in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

Download OpenSSL toolkit

Acquire the OpenSSL toolkit with GemEngine support from Thales Customer Support.

> **NOTE:** The Doc ID for downloading the GemEngine v1.2 from support portal is KB0016309.

Set up F5 BIG-IP

Install and configure F5 BIG-IP LTM. Refer to F5 BIG-IP documentation for further information about installing and configuring F5 BIG-IP. The product documentation for BIG-IP LTM is available at the following site under the Product Manuals section: https://support.f5.com/csp/home.

> **NOTE:** BIG-IP TMOS with Luna HSM only supports IPv4. You also need to ensure that the BIG-IP system is licensed for "External Interface and Network HSM."

> **NOTE:** If you install the Luna Network HSM (external HSM) on a system with a FIPS card (internal HSM) installed, the Luna Network HSM takes precedence. You cannot use the Luna Network HSM on a BIG-IP system that is running another external HSM.

Integrating Luna HSM with F5 BIG-IP

To integrate Luna HSM with F5 BIG-IP system complete the following:

> Configure Luna Client with F5 BIG-IP

> Generate a key/certificate Using traffic manager shell (tmsh)

> Configure a client SSL profile to use an external HSM key and certificate

> Import a pre-existing Luna HSM key into the BIG-IP

> Delete a key from the BIG-IP system

Configure Luna Client with F5 BIG-IP

To configure Luna Client with BIG-IP system complete one of the following tasks:

> Add Luna Client to BIG-IP System using automated script

> Add Luna Client to BIG-IP System manually

Add Luna Client to BIG-IP System using automated script

> **NOTE:** Follow these steps if you are using Luna HSM and adding Luna Client 7.1 to the Big-IP system using the automated script. For all other Luna Client versions, refer to Add Luna Client to the Big-IP System manually section.

To add the Luna Client to the BIG-IP System using automated script, you need to obtain the software tarball from Thales Support. To add the Luna Client to the BIG-IP system:

1. Log in to the command-line interface of the BIG-IP system using an account with administrator privileges.
2. Create a directory under the **/shared** directory named **safenet_install**.

   ```
   # mkdir /shared/safenet_install
   ```

3. Copy the Luna Client software tarball to the **/shared/safenet_install** directory.

   > **NOTE:** If you are setting up the Luna client on a VIPRION system, you only need to run the configuration script on the primary blade. The system propagates the configuration to the additional active blades following installation.

4. You can proceed to step 5 directly if you are not installing Luna client on a VIPRION system or if you are using a self IP address to communicate with the HSM. Otherwise, first you need to disable the ip check on the HSM using Luna Shell (LunaSH) and then proceed to step 5:

   ```
   # ntls ipcheck disable
   # service restart ntls
   ```

   > **NOTE:** This step allows the same certificate to be used from multiple IP addresses for communicating with HSM from multiple blades.

5. Install and register the Luna client on the BIG-IP system, using one of the following parameters:

   - Parameters for a standard installation or on the standalone or primary blade of a VIPRION system.

     ```
     # nethsm-safenet-install.sh --hsm_ip_addr=<luna_sa_device_IP_address> --
     image=<Luna_x.x_Client_Software .tar >
     ```

     The following example sets up the Luna Client v7.1 where the Luna Network HSM has an IP address of 10.164.74.111:

     ```
     # nethsm-safenet-install.sh --hsm_ip_addr=10.164.74.111 --image= Luna_7.1_
     Client_ Software.tar
     ```

     The system will prompt for Luna SA admin password and partition password.

     From Luna v7.x onwards, you need to initialize the partition and CO/CU user roles using root before entering the password. After initializing the partition and user roles enter the CO password and press Enter.

     > **NOTE:** The VIPRION system propagates the configuration to additional active blades, but you need to reload the PATH environment variable on any blades with already-open sessions: `source ~/.bash_profile`

   - Parameters when multiple HSMs are configured as an HA group.

```
# nethsm-safenet-install.sh --hsm_ip_addr="<SafeNet HSM1_IP_address>
<SafeNet HSM2_IP_address>" --hsm_ha_group=<Label name for the SafeNet HSM HA
group> --image=<Luna_x.x_Client_Software.tar>
```

The following example sets up the Luna Client v7.1 for an HA group named F5_Luna_HA where the Luna Network HSMs in the group have IP addresses of 10.10.10.100 and 10.10.10.101:

```
# nethsm-safenet-install.sh --hsm_ip_addr="10.10.10.100 10.10.10.101" --
hsm_ha_group=luna_ha_test --image=Luna_7.1_Client_Software.tar
```

Install all components when prompted during the installation. You need to register your client IP address with the Luna Network HSM and assign the Luna Client to a previously defined HSM partition.

You need to initialize the partition and CO/CU user roles using root before entering the partition password. Use the same password for all HA members. After initializing the partition and user roles, enter the CO password and press Enter.

> **NOTE:** By default, the script sets up the Luna client software to use 20 threads. To adjust this number, run this command before you restart the pkcs11d service: `tmsh sys crypto fips external-hsm num-threads <integer>`. Note that changing the number of threads affects performance.

Set up the Luna Client on a newly added or activated blade

After you set up the Luna Client on the primary blade of a VIPRION system, the system propagates the configuration to the additional active blades. If you subsequently add a secondary blade, activate a disabled blade, or power on a powered-off blade, you need to run a script on the new secondary blade. To set up the Luna Client on a newly added or activated blade:

1. Log in to the command-line interface of the system using an account with administrator privileges.
2. Execute the following on any new or re-activated secondary blade:

   ```
   # safenet-sync.sh <HSM partition password> -v
   ```

3. If you make the new blade a primary blade before running the synchronization script, you need to run the regular client installation and registration procedure only on the new primary blade.

   ```
   # nethsm-safenet-install.sh
   ```

Add Luna Client to BIG-IP System manually

Follow these steps to configure Luna Client with BIG-IP system manually:

> Install pkcs11d patch for Luna Cloud HSM

> Configure Luna Client with BIG-IP System

> Configure SafeNet as external-hsm

> Add Partition Information to BIG-IP System

Install pkcs11d patch for Luna Cloud HSM

> **NOTE:** Skip this section, if you are using Luna HSM. Doc IDs for downloading the pkcs11d fix patch from support portal is DOW0003489.

1. Mount the /usr directory in read-write mode.

   ```
   # mount -o remount,rw /usr
   ```

2. Take a backup of the existing pkcs11d configuration file so that it can be recovered again.

   ```
   # cp /usr/bin/pkcs11d /shared/pkcs11d_bk
   ```

3. Download the pkcs11d fix patch and copy it to /shared directory:
4. Install the patch by running:

   ```
   # rpm -Uvh /shared/pkcs11d-14.1.0-0.0.118.x86_64.rpm –force
   ```

5. Remount the /usr directory in read-only mode to prevent further modification.

   ```
   # mount -o remount,ro /usr
   ```

6. Restart pkcs11 service to apply the changes.

   ```
   # bigstart restart pkcs11d
   ```

Configure Luna Client with BIG-IP System

> **NOTE:** If you are using full client then ensure that Luna client is installed in /usr directory and partition is assigned to the client.

1. Mount the /usr directory in read-write mode.

   ```
   # mount -o remount,rw /usr
   ```

2. Copy the GemEngine library from OpenSSL toolkit to /usr/lib64/openssl/engines.

   ```
   # cp ./builds/linux/rhel/64/1.0.2/libgem.so /usr/lib64/openssl/engines/
   ```

3. Create a lunasa directory /shared/safenet/lunasa

   ```
   # mkdir -p /shared/safenet/lunasa
   ```

4. Create link for lunaclient to /shared/safenet/lunasa.

   ```
   # ln –sf <luna_client_installed_directory>/* /shared/safenet/lunasa
   ```

   For Full Client:

   ```
   ln -sf /usr/safenet/lunaclient/* /shared/safenet/lunasa
   ```

   For Minimal Client:

   ```
   ln –sf ~/bigip_dpodclient/* /shared/safenet/lunasa/
   ```

   where bigip_dpodclient is the directory where you extracted minimal client package.

5. Now open and modify the Chrystoki.conf file. If you are using full client package this file is located at /etc directory and if you are using minimal client package this file is located at /shared/safenet/lunasa directory.

   a. Modify the Chrystoki2 and Misc sections.

   ```
   Chrystoki2 = {
   LibUNIX64 = /shared/safenet/lunasa/lib/libCryptoki2.so;
   }
   Misc = {
   Apache = 0;
   ```

```
PE1746Enabled = 1;
 ………
}
```

b. Create a new GemEngine section with the indicated values.

```
GemEngine = {
EnableDsaGenKeyPair = 1;
EnableRsaGenKeyPair = 1;
DisablePublicCrypto = 1;
EnableRsaSignVerify = 1;
EnableLoadPubKey = 1;
EnableLoadPrivKey = 1;
DisableCheckFinalize = 1;
DisableEcdsa = 1;
DisableDsa = 0;
DisableRand = 0;
EngineInit = "<token_label>":0:0:passfile=/shared/safenet/lunasa/passfile;
EnableLoginInit = 1;
LibPath64 = /shared/safenet/lunasa/lib/libCryptoki2_64.so;
}
```

6. If you are using full client package, copy /etc/Chrystoki.conf to /shared/safenet/lunasa/. Skip this step in case you are using minimal client package.

```
# cp /etc/Chrystoki.conf /shared/safenet/lunasa/
```

7. If you are using minimal client package, copy /shared/safenet/lunasa/Chrystoki.conf to /etc. Skip this step for full client package.

```
# cp /shared/safenet/lunasa/Chrystoki.conf /etc
```

8. Adjust the permission of the Chrystoki.conf file.

```
# restorecon -R /shared/safenet

# chmod 644 /shared/safenet/lunasa/Chrystoki.conf
```

9. If you are using minimal client package, create a lib directory and copy the crypto libraries into the created directory. Skip this step for full client package.

```
# mkdir /shared/safenet/lunasa/lib

# cp /shared/safenet/lunasa/libs/64/libCryptoki2.so /shared/safenet/lunasa/lib/
libCryptoki2_64.so
```

10. Create the link for Luna Crypto Library.

```
# ln -sf /shared/safenet/lunasa/lib/libCryptoki2_64.so
/usr/lib/libCryptoki2_64.so

# ln -sf /shared/safenet/lunasa/lib/libCryptoki2_64.so /usr/lib/libCryptoki2.so
```

11. Create a password file to store the partition password. This file is used for the password when gemengine is called. For demonstration, we are using *userpin1* as the partition password.

    ```
    # echo userpin1 > passfile
    ```

12. Now install pkcs11d to the BIG-IP system.

    ```
    # bigstart add pkcs11d
    # bigstart stop pkcs11d
    # bigstart add --default pkcs11d
    ```

13. Remount the /usr directory in read-only mode to prevent further modification.

    ```
    # mount -o remount,ro /usr
    ```

Configure SafeNet as the external-hsm

You must add SafeNet as external-hsm vendor to BIG-IP System. To configure SafeNet as the external-hsm:

1. Set the vendor name to SafeNet.

   ```
   # fipskey.nethsm --hsm=Safenet
   ```

2. Configure the vendor name and partition password in tmsh.

   ```
   # tmsh create sys crypto fips external-hsm vendor safenet password
   <partition_password>
   ```

3. Restart the services to apply the changes.

   ```
   # bigstart start pkcs11d
   # bigstart restart tmm
   ```

Add Partition Information to BIG-IP System

You must add the partition information so that Traffic Manager Shell (tmsh) automatically uses the partition name and password when generating keys. There are two ways to add partition information:

- Add partition information using command line
- Add partition information using the web console

> **NOTE:** Before adding partition information using web console you must ensure that the external hsm vendor must be safenet. You can check it by running "`tmsh -a list sys crypto fips external-hsm vendor | grep vendor | tr -s ' ' | cut -d ' ' -f 3`" .If its output is "`safenet`" go ahead, If not then verify again all the previous steps.

Add partition information using command line

To add partition information using command line, run:

```
# tmsh -a create sys crypto fips nethsm-partition <partition_name> password
<partition_password>
```

Add partition information using the web console

To add partition information using the web console:

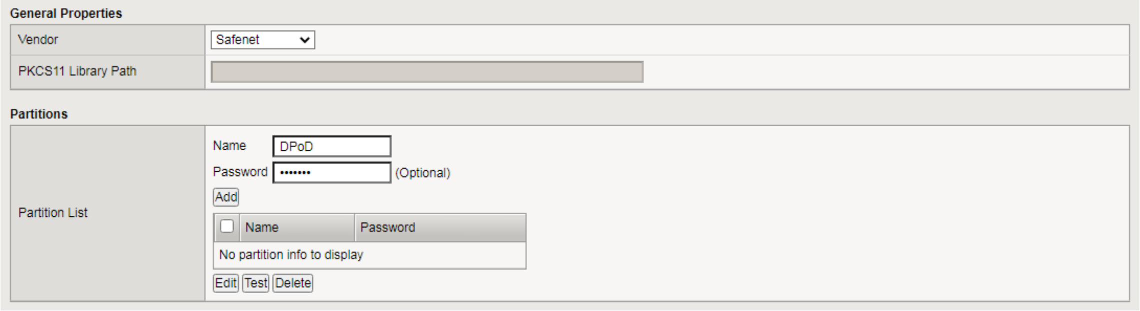
1. Open web console https://<big-ip_address>

2. On the Main tab, click **System** > **Certificate Management** > **HSM Management** > **External HSM**.

   The External HSM page will appear on your screen.

3. Select **Safenet** from **Vendor** and add the following values:

   - **Name**:<partition name>
   - **Password**:<partition password>



General Properties

Vendor: Safenet

PKCS11 Library Path:

Partitions

Partition List

Name: DPoD

Password: ••••••• (Optional)

Add

□	Name	Password
No partition info to display		

Edit Test Delete

4. Click **Add**. The partition is added.
5. Click **Update** to save the changes.
6. Go to **System**, click **Services,** and restart the **pkcs11d** service.

> **NOTE:** After adding partition information, verify that partition is listed using the `tmsh -a list sys crypto fips nethsm-partition` command.

Generate a key/certificate Using traffic manager shell (tmsh)

To generate a key/certificate using traffic manager shell, you need to complete anyone of the following task:

> Create a self-signed digital certificate using tmsh

> Create a self-signed digital certificate using web console

> Request a certificate from a certificate authority

Create a self-signed digital certificate using tmsh

Use the Traffic Management Shell (**tmsh**) to generate a key and certificate. To generate a key/certificate using tmsh:

1. Log in to the command-line interface of the system using an account with administrator privileges.
2. Open the **tmsh**.

   ```
   # tmsh
   ```

3. Generate the key.

   ```
   create sys crypto key <key_name> gen-certificate common-
   name <cert_name> security-type nethsm nethsm-partition-name <partition_name>
   ```

   The following example generates a key on HSM named **test_key** and a certificate named **test_safenet.com** with the security type **nethsm** on the partition **HA**.

   ```
   create sys crypto key test_key gen-certificate common-name test_safenet.com
   security-type nethsm nethsm-partition-name HA
   ```

4. Verify that the key was created.

   ```
   list sys crypto key test_key.key
   ```

   Information about the key displays:

   ```
   sys crypto key test_key {
   key-id c31fa09a744caa9a558612b303eb0719
   key-size 2048
   key-type rsa-private
   security-type nethsm
   }
   ```

   When you generate a key/certificate using **tmsh**, the system creates a HSM private key. It also creates a local key, which points to the HSM key residing in the HSM.

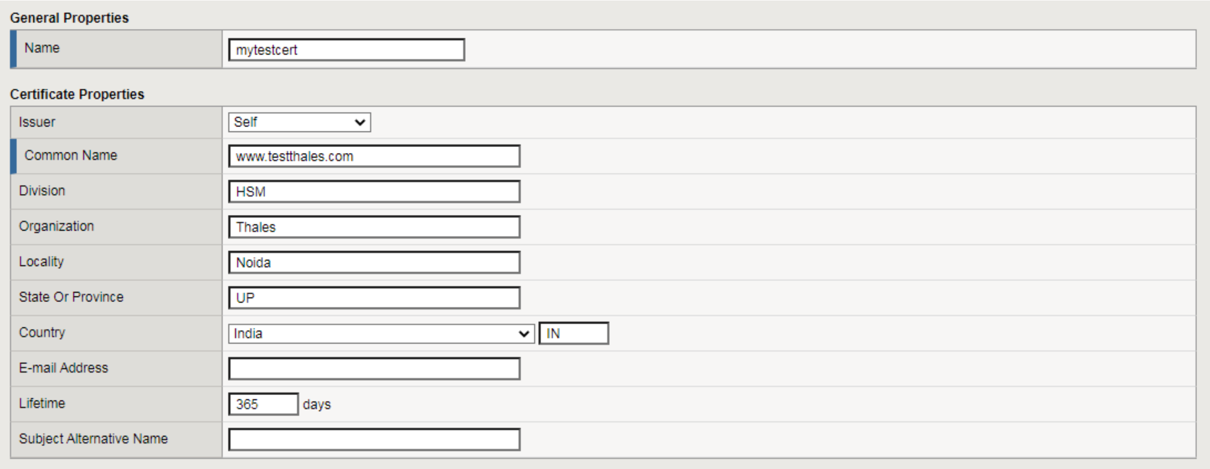
Create a self-signed digital certificate using web console

Use the web console to generate a key and certificate. To generate a key/certificate using web console:

1. On the Main tab, click **System** > **Certificate Management** > **Traffic Certificate Management**.

   The Traffic Certificate Management page will appear on your screen.

2. Click **Create**.



General Properties

Name	mytestcert

Certificate Properties

Issuer	Self
Common Name	www.testthales.com
Division	HSM
Organization	Thales
Locality	Noida
State Or Province	UP
Country	India IN
E-mail Address	
Lifetime	365 days
Subject Alternative Name	

   a. In the **Name** field, type a unique name for the SSL certificate.

   b. From the **Issuer** list, select **Self**.

   c. In the **Common Name** field, type a name.

      This is typically the name of a web site, such as www.siterequest.com.

   d. In the **Division** field, type your department name.

   e. In the **Organization** field, type your company name.

   f. In the **Locality** field, type your city name.

   g. In the **State or Province** field, type your state or province name.

   h. From the **Country** list, select the name of your country.

   i. In the **E-mail Address** field, type your email address.

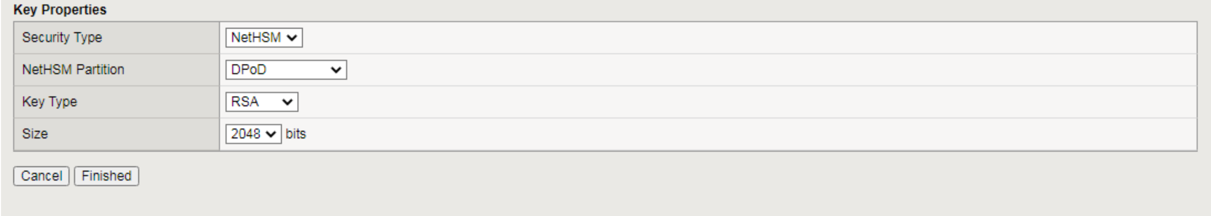
j. In the **Lifetime** field, type a number of days, or retain the default, **365**.

k. In the **Subject Alternative Name** field, type a name. This name is embedded in the certificate for X509 extension purposes. By assigning this name, you can protect multiple host names with a single SSL certificate.

l. From the **Security Type** list, select **NetHSM**.

m. From the **Key Type** list, **RSA** is selected as the default key type.

n. From the **Size** list, select a size, in bits.



Key Properties

Security Type	NetHSM
NetHSM Partition	DPoD
Key Type	RSA
Size	2048 bits

o. Click **Finished**.

Request a certificate from a certificate authority

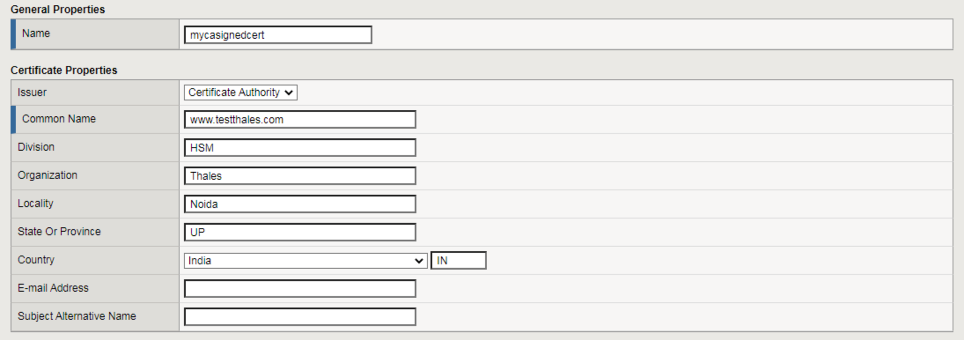
Generate a certificate signing request (CSR) that can then be submitted to a third-party trusted certificate authority (CA).

> **NOTE:** Please consult the CA to determine the specific information required for each step in this task.

To request a certificate from a certificate authority:

1. On the Main tab, click **System** > **Certificate Management** > **Traffic Certificate Management**. The Traffic Certificate Management page will appear on your screen.

2. Click **Create**.



General Properties

Name	mycasignedcert

Certificate Properties

Issuer	Certificate Authority
Common Name	www.testthales.com
Division	HSM
Organization	Thales
Locality	Noida
State Or Province	UP
Country	India IN
E-mail Address	
Subject Alternative Name	

a. In the **Name** field, type a unique name for the SSL certificate.

b. From the **Issuer** list, select **Certificate Authority**.

c. In the **Common Name** field, type a name.

This is typically the name of a web site, such as www.siterequest.com.

d. In the **Division** field, type your department name.

e. In the **Organization** field, type your company name.

f. In the **Locality** field, type your city name.

g. In the **State or Province** field, type your state or province name.

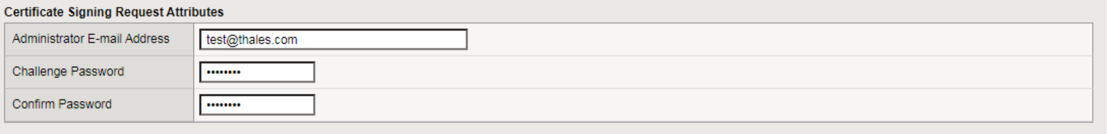
h. From the **Country** list, select the name of your country.

i. In the **E-mail Address** field, type your email address.

j. In the **Subject Alternative Name** field, type a name. This name is embedded in the certificate for X509 extension purposes. By assigning this name, you can protect multiple host names with a single SSL certificate.

k. In the **Challenge Password** field, type a password.

l. In the **Confirm Password** field, re-type the password you typed in the **Challenge Password** field.



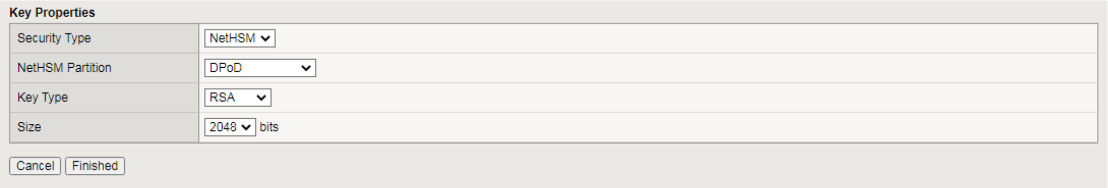
Certificate Signing Request Attributes

Administrator E-mail Address	test@thales.com
Challenge Password	••••••••
Confirm Password	••••••••

m. From the **Security Type** list, select **NetHSM**.

n. From the **Key Type** list, **RSA** is selected as the default key type.

o. From the **Size** list, select a size, in bits.



Key Properties

Security Type	NetHSM
NetHSM Partition	DPoD
Key Type	RSA
Size	2048 bits

p. Click **Finished**.

The Certificate Signing Request screen displays.

3. Perform one of the following tasks to download the request into a file on your system.

   - In the Request Text field, copy the certificate.
   - For Request File, click the button.

4. Follow the instructions on the relevant certificate authority web site for either pasting the copied request or attaching the generated request file.

5. Click **Finished**. The Certificate Signing Request page will appear on your screen.

6. Submit the generated certificate signing request to a trusted certificate authority for signature.

Configure a Client SSL Profile to Use an External HSM key and certificate

After you have added the Luna HSM key and certificate to the BIG-IP system configuration, you can use the key and certificate as part of a client SSL profile. This task describes using the browser interface. Alternatively, you can use the Traffic Management Shell (**tmsh**) command-line utility. To configure a client SSL profile to use an external HSM key and certificate:

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.

   The Client screen opens.

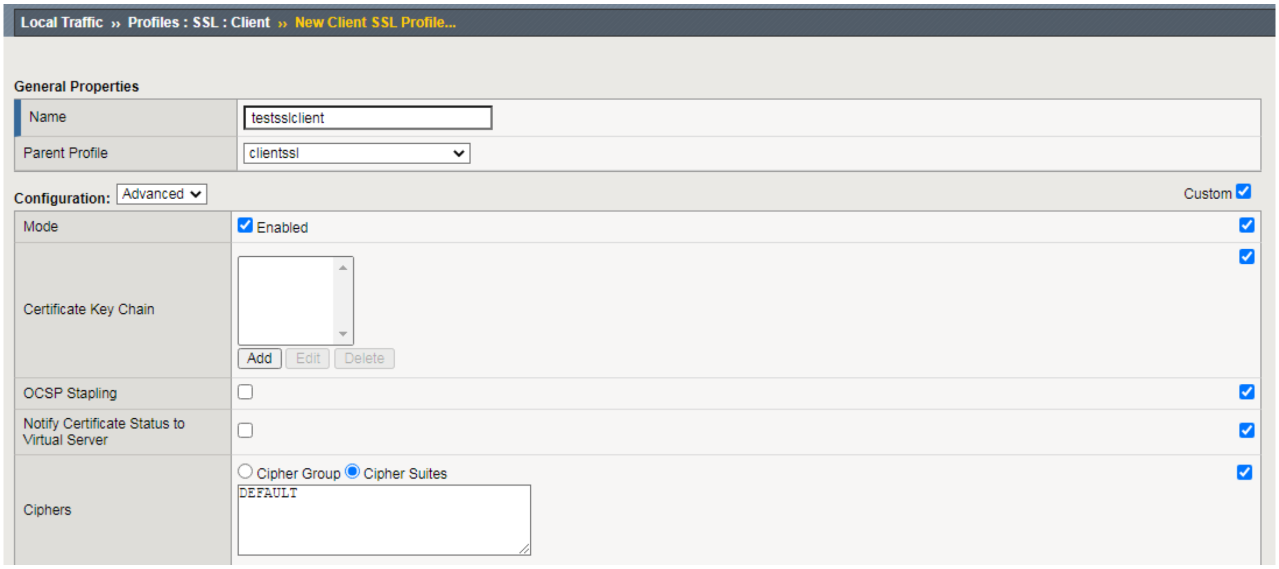
2. Click **Create**.

   The New Client SSL Profile page will appear on the screen.

3. In the Name field, type a name for the profile.

4. From the Parent Profile list, select **clientssl**.

5. From the Configuration list, select **Advanced**. This selection makes it possible for you to modify additional default settings.



Local Traffic » Profiles : SSL : Client » New Client SSL Profile...

General Properties

Name	testsslclient
Parent Profile	clientssl

Configuration: Advanced   Custom ☑

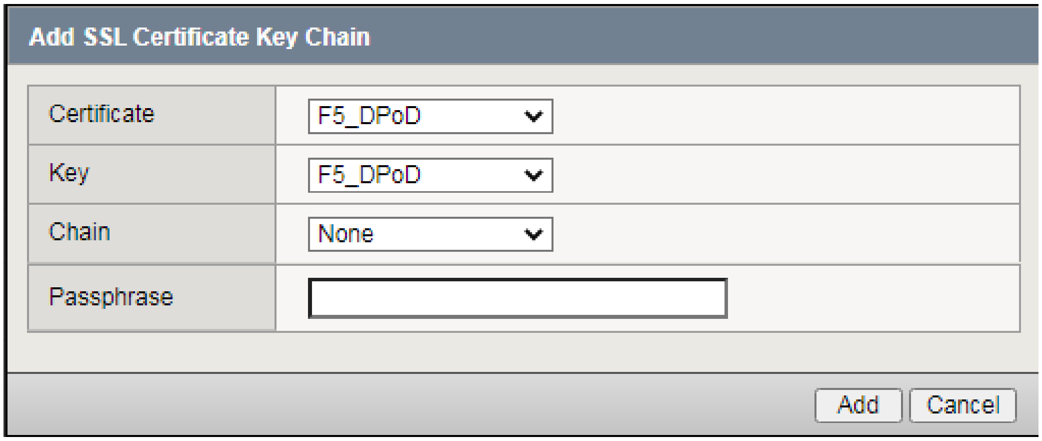
Mode	☑ Enabled	☑
Certificate Key Chain	Add Edit Delete	☑
OCSP Stapling	□	☑
Notify Certificate Status to Virtual Server	□	☑
Ciphers	○ Cipher Group ● Cipher Suites DEFAULT	☑

6. For the Configuration area, select the **Custom** check box.

   The settings in the Configuration area become available for modification.

7. Using the **Certificate Key Chain** setting, specify one or more certificate key chains:

   - From the Certificate list, select the name of a certificate that you imported.
   - From the Key list, select the name of the key that you imported.
   - From the Chain list, select the chain that you want to include in the certificate key chain.



Add SSL Certificate Key Chain

Certificate	F5_DPoD
Key	F5_DPoD
Chain	None
Passphrase	

   - Click **Add**.

8. Click **Finished**.

   After you have created the client SSL profile, you must assign the profile to a virtual server, so that the virtual server can process SSL traffic according to the specified profile settings.

Import a pre-existing Luna HSM key into the BIG-IP

A pre-existing key on the Luna HSM can be imported to use with BIG-IP.

> **NOTE:** F5 BIG-IP does not support the ability to import/migrate any existing keys from BIG-IP to HSM.

To import a pre-existing Luna HSM key into the BIG-IP:

1. On the Main tab, click **System** > **Certificate Management** > **Traffic Certificate Management** > **SSL Certificate List** > **Import**.

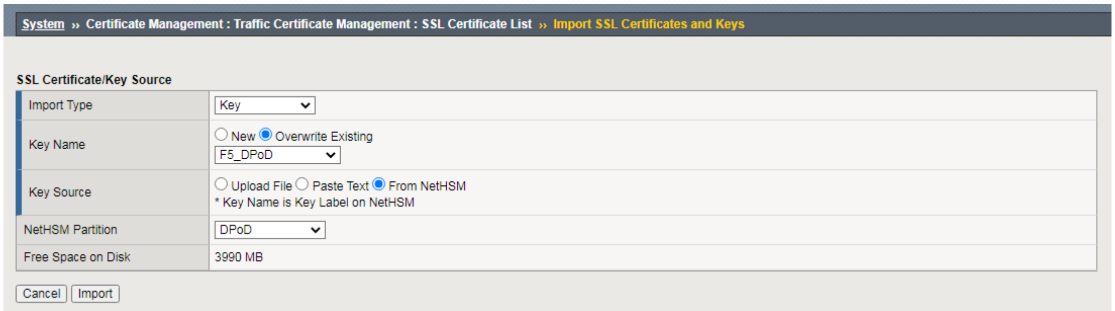
   The SSL Certificate/Key Source page will appear on your screen.

2. Within **Import Type**, select **Key**. The key name should be the same as the Luna HSM key label.

3. Within **Key Name**, select **Overwrite Existing** and from the drop-down menu, select the key you would like to overwrite.

4. Within Key Source, select **From NetHSM**.

   For this option to be available, the system must have External HSM licensed, and SafeNet External HSM is configured.


System » Certificate Management : Traffic Certificate Management : SSL Certificate List » Import SSL Certificates and Keys
Cancel
Import

SSL Certificate/Key Source

Import Type	Key
Key Name	○ New ● Overwrite Existing F5_DPoD
Key Source	○ Upload File ○ Paste Text ● From NetHSM * Key Name is Key Label on NetHSM
NetHSM Partition	DPoD
Free Space on Disk	3990 MB

5. Click **Import**.

   You can also import an existing key by using tmsh commands:

```
# tmsh install sys crypto key nethsm_key_label from-nethsm security-type nethsm
```

   or

```
# tmsh install sys crypto key nethsm_key_label from-nethsm
```

   Use the NetHSM key label as the key name. For example:

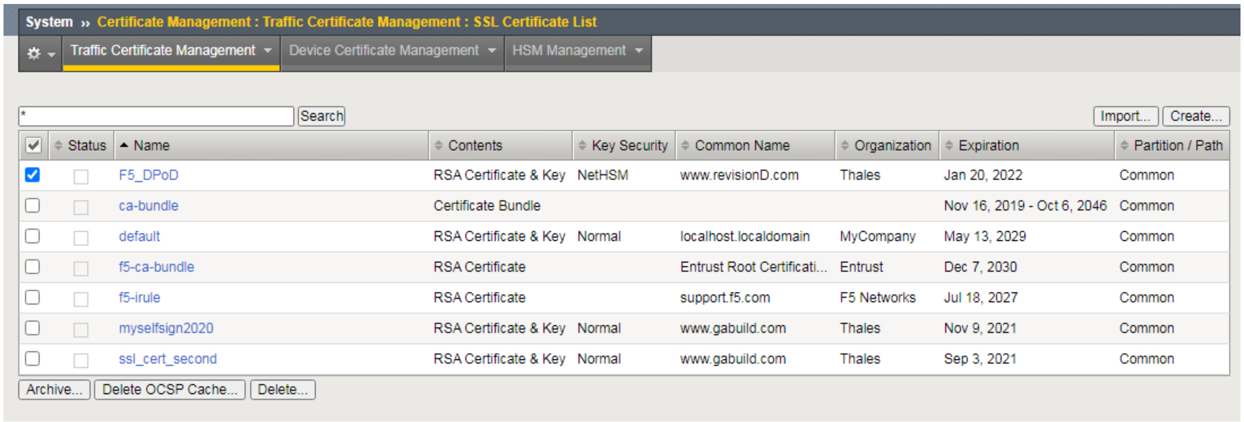
```
root@(ssl8519)(cfg-sync Standalone)(Active)(/Common)(tmos)# install sys crypto
key

nethsm_key_label (tab)

Options:

from-editor        from-nethsm

Properties:

from-local-file    from-url

root@(ssl8519)(cfg-sync Standalone)(Active)(/Common)(tmos)# install sys crypto
key  nethsm_key_label from-nethsm security-type nethsm
```

Delete a Key from the BIG-IP system

You perform this task to delete an existing key from the BIG-IP. To delete a key from the BIG-IP:

1. On the Main tab, click **System** > **Certificate Management** > **Traffic Certificate Management**.

   The Traffic Certificate Management screen will appear on the screen.


System » Certificate Management : Traffic Certificate Management : SSL Certificate List
Traffic Certificate Management
Device Certificate Management
HSM Management
*
Search
Import...
Create...
Archive...
Delete OCSP Cache...
Delete...

☑	Status	Name	Contents	Key Security	Common Name	Organization	Expiration	Partition / Path
☑	□	F5_DPoD	RSA Certificate & Key	NetHSM	www.revisionD.com	Thales	Jan 20, 2022	Common
□	□	ca-bundle	Certificate Bundle				Nov 16, 2019 - Oct 6, 2046	Common
□	□	default	RSA Certificate & Key	Normal	localhost.localdomain	MyCompany	May 13, 2029	Common
□	□	f5-ca-bundle	RSA Certificate		Entrust Root Certificati...	Entrust	Dec 7, 2030	Common
□	□	f5-irule	RSA Certificate		support.f5.com	F5 Networks	Jul 18, 2027	Common
□	□	myselfsign2020	RSA Certificate & Key	Normal	www.gabuild.com	Thales	Nov 9, 2021	Common
□	□	ssl_cert_second	RSA Certificate & Key	Normal	www.gabuild.com	Thales	Sep 3, 2021	Common

2. From the **SSL Certificate List**, select the check box next to the key you wish to delete.
3. Click **Delete**. The key you selected is deleted from BIG-IP. The key stored in the Luna HSM is not deleted.

This completes the integration of Luna HSM with F5 BIG-IP.

Contacting Customer Support

If you encounter a problem during this integration, contact your supplier or Thales Customer Support. Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.